UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/668,421	09/22/00	ANANDA	M 81045 P.3D3

EXAMINER	
SOUGH, H	
ART UNIT	**PAPER NUMBER**
2161	5

022804
THE HECKER LAW GROUP
1925 CENTURY PARK EAST
SUITE 2300
LOS ANGELES CA 90067

TM02/0813

DATE MAILED: 08/13/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	Applicant(s)
09/668,421	Ananda
Examiner	**Art Unit**
Huyng S. Sough	2161

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *three* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-67* is/are pending in the application.

4a) Of the above, claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-67* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9) ☒ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *22 Sep 2000* is/are objected to by the Examiner.

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a) ☐ All b) ☐ Some* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)
16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). _____
18) ☐ Interview Summary (PTO-413) Paper No(s). _____
19) ☐ Notice of Informal Patent Application (PTO-152)
20) ☐ Other:

Drawings

1. The drawings are objected to by the Examiner for numerous informalities:

For example,

• They are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "108" (FIG. 1) and "114" (FIG. 20) have both been used to designate "keyboard".

• They are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "114" has been used to designate both "coupling" (FIG. 1) and "keyboard" (FIG. 20); "102" has been used to designate both "user computer" (FIG. 1) and "CPU" (FIG. 20).

• They are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: "118" (page 28, line 3), "15014" (page 28, line 8), "15015" (page 28, line 9), "15016" (page 28, line 23).

Applicant is advised to carefully review all the drawings for further needed corrections.

2. **A proposed drawing correction or corrected drawings are required in reply to this Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.**

Specification

3. The disclosure is objected to because of numerous informalities:

For example,

- Page 25, line 20, should "114" after "keyboard" be --108--?
- Page 26, line 14, should "114" after "Coupling" be --134--?
- Page 29, line 7, should "120" after "interface" be --10020--?
- Page 29, line 8, should "136A" after "link" be --10021--?
- Page 30, line 6, before "150", --system--should be inserted.
- Page 59, line 12, should "12" after "computer" be --122--?

Applicant is advised to carefully review the entire specification for further needed corrections.

Claim Objections

4. Claims **6-14, 18, 19, and 42-62** are objected to because of the following informalities:

- Claim 6, line 2, "a postal indicia" should be changes to either --postal indicia-- or --a postal indicium--.
- Claim 18, line 1, "an indicia" should be changes to either --indicia-- or --an indicium--.
- Claim 42, line 6, "an indicia" should be changes to either --indicia-- or --an indicium--.

Applicant is advised to carefully review all the claims for further needed corrections.

Claim Rejections - 35 U.S.C. § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims **1-41, 49-51, 56, 57, 59, 60, 64, and 65** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claim 1, line 8-9, "said printing software" does not have proper antecedent basis.
- Claim 12, line 2, should "user information" be either --said user information-- or --the user information--?
- Claim 17, line 3, "said asynchronous header code" does not have proper antecedent basis.
- Claim 18, line 1, "said step of printing an indicia" does not have proper antecedent basis.

Line 3, "said printer" does not have proper antecedent basis.

- Claim 32, lines 10-11, "said first computer" and "said second computer" do not have proper antecedent basis, respectively.
- Claim 49, it is not clear whether "a password" in line 3 is the same "password" recited in line 3 of claim 44.

• Claims 56 and 57, before "communication" in line 1, --the-- or --said-- should be inserted, respectively.

• Claim 59, before "private" in line 1, --the-- or --said-- should be inserted.

• Claim 64, before "server" and "client" in line 2, "a" should be changed to --the-- or --said--, respectively.

• Claim 65, line 1, it is not clear whether "said system" is referring "an on-line postage system", "a client system", "a server system", or what?

Applicant is advised to carefully review all the claims for further needed corrections.

Claim Rejections - 35 U.S.C. § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims **1-7, 15, 16, and 32-36** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara (US PAT. 5,822,739) in view of Bosen et al. (Bosen hereinafter: US PAT. 5,060,263).

Kara discloses a secure on-line printing method, comprising:

establishing a communication link between a first computer and a second computer *(i.e., claim 27, the step of "coupling said first system to a second processor-based system")*;

executing a print software on said first computer, wherein said print software initiates a continuous communication link between said first computer and said second computer *(col. 6, lines 11-17)*;

sending a request from said print software to said second computer *(i.e., claim 27, the step of "transmitting said demand from said first system to said second system") for a print authorization*; and

said second computer sending a permission and information to the first computer in response to said request *(i.e., claim 27, the step of "transmitting said data packet from said second system to said first system"),* while said communication link is continuous *(col. 11, lines 13-18)*.

Further, Kara discloses a secure on-line postage metering method comprising the steps of:

a user computer establishing a communication link with a vendor computer *(i.e., claim 27, the step of "coupling said first system to a second processor-based system")*;

providing a printer connected to said user computer *(printer 24)*;

executing an on-line postage metering software on said user computer *(col. 6, lines 11-17)*;

said on-line postage metering software *(i.e., "Demand program")* sending a request for a print authorization for a postage amount *(col. 6, lines 4-7)* to said vendor computer *(i.e., claim 27, the step of "transmitting said demand from said first system to said second system")*;

said vendor computer accessing a database to verify fund availability to cover said postage amount *(col. 13, lines 31-45)*;

said vendor computer sending a permission and image information to said first computer in response to said request *(i.e., claim 27, the step of "transmitting said data packet from said second system to said first system")*; and

said on-line postage metering software sending said image information to said printer *(i.e., "Demand program" decrypting the received data packet for printing)*.

Re claim 1: Kara does not explicitly disclose the use of a dynamic password and the step of verifying the dynamic password for terminating the print software when said communication link is not continuous. However, Bosen teaches the use of a dynamic password to control access to protected system and the step of verifying the dynamic password for terminating unauthorized access (see the abstract, column 1-5, and FIGURE 3). Thus, it would have been within the level of ordinary skill in the art to modify the method of Kara by adopting the teaching of Bosen to provide the enhanced security to the claimed method.

Re claim 2: Kara discloses that said value-bearing information *(i.e., "data packet")* is used for printing an image *(i.e., "postage indicia")*.

Re claims 3, 4, and 5: Kara discloses that a request, a permission and information are encrypted *(col. 6, lines 17-22)*.

Re claim 6: Kara discloses said information comprising an image of a postal indicium *(col. 6, lines 40-42)*.

Re claim 7: Kara discloses said request for the print authorization comprising a postage amount *(col. 6, lines 4-7)*.

Re claims 15, 16, and 32: Kara does not explicitly disclose that the software uses an asynchronous header with a dynamic password to initiate a continuous communication link between the first computer and the second computer and said on-line postage metering software sends said image information to said printer while said communication link is continuous. However, Bosen teaches the use of an asynchronous system with a dynamic password to control an unauthorized access to a protected system (see the abstract, column 1-5). Thus, it would have been within the level of ordinary skill in the art to modify the method of Kara by adopting the teaching of Bosen to provide an enhanced security to the claimed method. Further, the examiner takes official notice of both motive and modification necessary for the step of sending said image information to said printer while said communication link is continuous. More specifically, this feature is well known in the data processing art to transfer confidential data securely and the abrupt disconnection of a secure link signifies that there is a possibility of breaching of security transferring sensitive data. Thus, it would have been within the level of ordinary skill in the art to employ this well-known feature for the Method of Kara

to prevent theft of confidential information (e.g., credit card or debit account number) or fraudulent use of postage.

Re claims 33, 34, and 35: Kara discloses said online postage metering software sending a request comprising encrypting said request and said vendor computer sending a permission and image information including encrypting said permission and said image information *(col. 6, lines 17-22)*.

Re claim 36: Neither Kara nor Bosen explicitly discloses the step of said on-line postage metering software disabling a print spooler of said printer. However, the examiner takes official notice of both motive and modification necessary for this feature. More specifically, this feature is well known in the data processing art to transfer confidential data securely and the abrupt disconnection of a secure link signifies that there is a possibility of breaching of security transferring sensitive data. Thus, it would have been within the level of ordinary skill in the art to employ this well-known feature for the system of Kara to prevent theft of confidential information (e.g., credit card or debit account number) or fraudulent use of postage.

9. Claims **8-14, 20-23, and 37-41** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara in view of Bosen as applied to claims 5, 7 and 36 above, and further in view of IBM Technical Disclosure Bulletin (IBM hereinafter: "Encrypted Data Transmission

with Dynamic Key Renewal", IBM Technical Disclosure Bulletin, August 1992, Vol. 35, Issue 3, pp 62-62).

Re claims 8, 9, 37, and 38: Neither Kara nor Bosen explicitly discloses that the dynamic password generation is based upon the delivery destination information, the postage amount, or a time on the first computer. However, IBM teaches the use of dynamic passwords (i.e., keys) being generated repeatedly for each data transmission to prevent unauthorized use of information exchanged between a central site and a decentral site. Thus, it would have been within the level of ordinary skill in the art to further modify the method of Kara and Bosen by adopting the teaching of IBM to prevent unauthorized use of information (i.e., the delivery destination information, the postage amount, a time on the first computer, a user information, the ticket price, the check amount, the coupon amount, and etc.) exchanged between the central site and the decentral site.

Re claims 10 and 39: Kara discloses that said step of said print (or said on-line postage metering) software sending a request for a print authorization is in response to a command from a user *(col. 3, lines 16-19)*.

Re claims 11 and 40: Neither Kara nor Bosen explicitly discloses that the dynamic password generation is based upon a user information. However, IBM teaches the use of dynamic passwords (i.e., keys) being generated repeatedly for each data transmission to prevent unauthorized use of information exchanged between a central site and a decentral site. Thus, it would have been within the level of ordinary skill in the art to further modify the

method of Kara and Bosen by adopting the teaching of IBM to prevent unauthorized use of information (i.e., the delivery destination information, the postage amount, a time on the first computer, a user information, the ticket price, the check amount, the coupon amount, and etc.) exchanged between the central site and the decentral site.

Re claims 12 and 13: Kara discloses said second computer comprising a database containing user information, wherein said user information comprises financial information associated with said user *(col. 13, lines 31-45. It is well known in the art to keep user's credit or debit account in a database)*.

Re claim 14: Kara discloses said sending a request to said second computer further comprises accessing said user information to verify fund availability to cover said postage amount *(col. 13, lines 31-45)*.

Re claims 20 and 21: Kara discloses said information comprising ticket information and said request comprises a ticket price *(col. 15, lines 27-32)*.

Re claim 22: Neither Kara nor Bosen explicitly discloses that the dynamic password generation is based upon the ticket price. However, IBM teaches the use of dynamic passwords (i.e., keys) being generated repeatedly for each data transmission to prevent unauthorized use of information exchanged between a central site and a decentral site. Thus, it would have been within the level of ordinary skill in the art to further modify the method of Kara and Bosen by adopting the teaching of IBM to prevent unauthorized use of information (i.e., the delivery destination information, the postage amount, a time on the first computer, a user information,

the ticket price, the check amount, the coupon amount, and etc.) exchanged between the central site and the decentral site.

Re claim 23: Kara discloses that said second computer sends a permission to said first computer in response to said request, said second computer accessing a user's financial information to verify funds availability to cover the ticket price *(col. 13, lines 31-45. If proper funding is available, said second computer sends permission to said first computer to use the Meter program)*.

Re claim 41: None of Kara, Bosen and IBM explicitly discloses the step of said on-line postage metering software sending a print cancel command to said printer when said communication link is interrupted. However, the examiner takes official notice of both motive and modification necessary for this feature. More specifically, this feature is well known in the data processing art to transfer confidential data securely and the abrupt disconnection of a secure link signifies that there is a possibility of breaching of security transferring sensitive data. Thus, it would have been within the level of ordinary skill in the art to employ this well-known feature for the method of Kara, Bosen and IBM to prevent theft of confidential information (e.g., credit card or debit account number) or fraudulent use of postage.

10. Claims **17, 18, and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara in view of Bosen as applied to claim 16 above, and further in view of Walker et al. (Walker hereinafter: US PAT. 4,991,208).

Re claim 17: Neither Kara nor Bosen explicitly discloses the use of a controller code which provides inputs to the asynchronous header code. However, Walker teaches the use of a controller code for a dynamic password *(column 1, lines 41-48)* to control an unauthorized access to the protected system. Thus, it would have been within the level of ordinary skill in the art to modify the method of Kara and Bosen by adopting the teaching of Walker to control an unauthorized access to the protected system.

Re claims 18 and 19: None of Kara, Bosen and Walker discloses the step of disabling the print spooler of the printer or said print software sending a print cancel command to said printer when said communication link disconnects. However, the examiner takes official notice of both motive and modification necessary for these features. More specifically, these features are well known in the data processing art to transfer confidential data securely and the abrupt disconnection of a secure link signifies that there is a possibility of breaching of security transferring sensitive data. Thus, it would have been within the level of ordinary skill in the art to employ these well-known features for the method of Kara, Bosen and Walker to prevent theft of confidential information (e.g., credit card or debit account number) or fraudulent use of postage.

11. Claims **42-56** and **58-60** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara.

Kara discloses a secure on-line postage management method comprising:

establishing a secure continuous communication link between a client system and a server system *(col. 6, lines 11-22)*;

said client system processing a user request for obtaining an indicium *(col. 6, lines 11-22)*;

said client system securely communicating said user request to said server system *(col. 6, lines 11-22)*;

said server system processing said user request *(col. 6, lines 37-43)*;

said server system securely communicating to said client system a response to said user request *(col. 6, lines 11-22)*;

said client system processing said response to obtain said indicium *(col. 6, lines 11-22, "decrypting the received data packet")*; and

said client system generating said indicium *(printing the desired postage indicia)*.

Re claim 42: Kara does not explicitly disclose that the client system generating an indicium while communication between the server system and the client system remains secure and continuous. However, in lines 6-21 of column 11 thereof, Kara discloses that the termination of the communications link could be terminated at any desirable time. Further, the examiner takes official notice of both motive and modification necessary for this feature. More specifically, these features are well known in the data processing art to transfer confidential data securely and the abrupt disconnection of a secure link signifies that there is a possibility of breaching of security transferring sensitive data. Thus, it would have been within the level of

ordinary skill in the art to employ these well-known features for the system of Kara to prevent theft of confidential information (e.g., credit card or debit account number) or fraudulent use of postage.

Re claim 43: Kara discloses that said client system securely communicating with said server system comprises authenticating a user by establishing a secured communication link between said client system and said server system and verifying the authenticity of information exchanged; and continuously monitoring said secured communication link to verify said authenticity of information exchanged *(col. 6, lines 11-22, "utilizing cryptographic key sets")*.

Re claims 44, 45, 46, 47, 48, 49, 50, 51, 52, and 53: Kara states the use of various security processes (col. 6, lines 11-22) without explicit disclosure of the specifically claimed features. However, the examiner takes official notice of both motive and modification necessary for these features. More specifically, these features are well known in the E-commerce art to prevent theft of confidential information (e.g., credit card or debit account number) or fraud. Thus, it would have been within the level of ordinary skill in the art to employ above well-known features for the system of Kara to prevent theft of confidential information (e.g., credit card or debit account number) or fraud.

Re claim 54: Kara discloses that said server system processing said user request takes place in a public network *("the Meter program")* and a private network *("the bank card company" of the user)* included within said server system.

Re claim 55: Kara discloses that said public network processes *("preparing data packet" by the "Meter program")* user requests independently from a said private network *(col. 13, lines 49-50, "credit account maintained at the local site and transmitted with the indicia request")* to protect the integrity of said server system.

Re claim 56: Kara discloses that communication between client system and server system is encrypted *(col. 6, lines 11-22)*.

Re claim 58: Kara does not explicitly disclose the step of disabling said client system from obtaining said indicium if said secure and continuous communication between client system and server system is discontinued. However, the examiner takes official notice of both motive and modification necessary for this feature. More specifically, these features are well known in the data processing art to transfer confidential data securely and the abrupt disconnection of a secure link signifies that there is a possibility of breaching of security transferring sensitive data. Thus, it would have been within the level of ordinary skill in the art to employ these well-known features for the system of Kara to prevent theft of confidential information (e.g., credit card or debit account number) or fraudulent use of postage.

Re claim 59: Kara discloses that said private network processes user request for making payments *(col. 13, lines 49-50, "credit account maintained at the local site and transmitted with the indicia request")*.

Re claim 60: Kara discloses that said private network processes user request for making payments further comprises communicating with a financial management system for

verification of availability of funds and fund transfer *(col. 13, lines 49-50, "credit account maintained at the local site and transmitted with the indicia request")*.

12. Claims **24, 25, 28, 29 and 31** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara in view of Bosen as applied to claims 1 and 5 above, and further in view of Edelmann et al. (Edelmann hereinafter: US PAT. 4,775,246).

Kara states that his invention "may be utilized to transmit any form of indicia." (Col. 15, lines 25-26) without explicitly disclosing the information comprising check information, coupon information or certificate information and the request comprising a check amount or a coupon amount. However, Edelmann shows various form of indicia *(e.g., postage, parcel service, tax stamps, checks writing, ticket, and other similar indicia: col. 5, lines 17-23)*. Thus, it would have been obvious to one of ordinary skill in the art to modify the method of Kara by employing the information comprising any known indicia as shown by Edelmann as desired to detect fraudulent imprints on documents that require verification and authentication of a user.

13. Claims **26 and 27** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara in view of Bosen and Edelmann as applied to claim 25 above, and further in view of IBM.

Re claim 26: None of Kara, Bosen or Edelmann explicitly discloses that the dynamic password generation is based upon the delivery destination information, the postage amount, a time on the first computer, a user information, the ticket price, the check amount, and the coupon amount. However, IBM teaches the use of dynamic passwords (i.e., keys) being

generated repeatedly for each data transmission to prevent unauthorized use of information exchanged between a central site and a decentral site. Thus, it would have been within the level of ordinary skill in the art to further modify the method of Kara, Bosen and Edelmann by adopting the teaching of IBM to prevent unauthorized use of information (i.e., the delivery destination information, the postage amount, a time on the first computer, a user information, the ticket price, the check amount, the coupon amount, and etc.) exchanged between the central site and the decentral site.

Re claim 27: Kara discloses that said second computer sends a permission to said first computer in response to said request further comprises the step of:

said second computer accessing a user's financial information to verify funds availability to cover the check amount and sending a permission to the first computer *(col. 13, lines 31-45. If proper funding is available, said second computer sends permission to said first computer to use the Meter program)*.

14. Claims **57 and 61-67** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kara in view of Information Based Indicia Program System Specification (IBIPSS hereinafter: October 9, 1996, The United states postal Service).

Kara discloses an on-line postage system for processing of user requests and obtaining postage indicia comprising:

a client system *(a first processor-based system)* for interfacing with a user;

a server system *(a second processor-based system)* in continuous and secure communication with said client system, comprising *(col. 6, lines 11-22)*:

a communication server for communicating with client system *(col. 7, lines 18-36)*;

a database server for storing user information *(col. 14, lines 24-30)*;

a transaction server for processing of requests communicated to said server system by said client system *(col. 14, lines)*;

a cryptographic device for encrypting communication between said client system and said server system *(col. 6, lines 20-23, i.e., "decrypting the received data packet" implies that the second processor-based system must have a cryptographic device)*;

a communication link with a financial management system for processing user payments *(col. 13, lines 45-50, i.e., "the provider will demand payment from the bank card company concurrent with the postage demand.")*.

Re claim 57: Kara does not explicitly disclose that communication between client system and server system is encrypted by a United States Postal Service compliant cryptographic device. However, as shown by IBIPSS *(see page 3-13, section 3.2.6.3)*, the open system server shall prompt the user to apply *(register)* for a postage meter license and update the license as required by the DMM. Thus, it would have been obvious to one of ordinary skill in the art to employ the client system and server system being encrypted by a United States Postal Service compliant cryptographic device to establish a communication link

with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user to satisfy the requirement.

Re claims 61 and 62: Kara does not explicitly disclose that said server system communicating with the United States Postal Service Central Meter Licensing System (USPS CMLS) for processing of user licensing information. However, as shown by IBIPSS *(see page 3-13, section 3.2.6.3)*, the open system server shall prompt the user to apply *(register)* for a postage meter license and update the license as required by the DMM. Thus, it would have been obvious to one of ordinary skill in the art to establish a communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user to satisfy the requirement.

Re claim 63: Kara does not explicitly disclose either a firewall for ensuring the integrity of said server system against potential unauthorized access or a communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user. However, as shown by IBIPSS *(see page 3-13, section 3.2.6.3)*, the open system server shall prompt the user to apply for a postage meter license and update the license as required by the DMM. Thus, it would have been obvious to one of ordinary skill in the art to establish a communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user to satisfy the requirement. Further, Kara states that the server system can be used by a plurality of remotely located client systems and the client system provides security system to prevent unauthorized utilization of the

postage metering system *(col. 4, lines 36-51)*. Of course, a firewall is one of the well-known security systems in the art and the use of this well-known feature at the server system would have been within the level of ordinary skill in the art, since it has been held that rearranging parts of an invention involves only routine skill in the art. *In re Japikse*, 86 USPQ 70.

Re claim 64: IBIPSS disclose the use of a system software down-loadable from said server system to said client system *(see page 3-3, section 3.2.1.1)* to ensure the proper installation and configuration of the user system. Thus, it would have been obvious to one of ordinary skill in the art to modify the system of Kara by adopting the teaching of IBIPSS to ensure the proper installation and configuration of the client system.

Re claim 65: Kara discloses that said server system is accessible through an Internet portal *(col. 7, lines 25-27)*.

Re claim 66: Kara discloses that said client system interfaces with at least one user *(col. 1, lines 22-29)*.

Re claim 67: Kara discloses that said client system comprises administration software *(i.e., a data communications program)* to monitor *(i.e., to maintaining a link, the data communication program has to monitor the system)* at least one client system.

Double Patenting

15. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same

invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

16. Claims 63-67 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 63-67 of co-pending Application No. 09/163,993. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

17. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

18. Claims 1-41 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-4, 6, 7, 12-14, 18-21, 23-25, 27-29, 31-36, 39, and 41 of co-pending Application No. 09/163,993 in view of Bosen,

Edelmann, IBM, Walker, and IBIPSS. The corresponding claims of co-pending Application No. 09/163,993 do not explicitly recite the same features as claimed in the instant application. However, as stated supra, in view of Bosen, Edelmann, IBM, Walker, and IBIPSS, it would have been within the level of ordinary skill in the art to modify the corresponding claims of co-pending Application No. 09/163,993 by adopting the teachings of Bosen, Edelmann, IBM, and IBIPSS to provide the enhanced security to the claimed method.

This is a provisional obviousness-type double patenting rejection.

19. Claims 42-62 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 42-62 of co-pending Application No. 09/163,993. Although the conflicting claims are not identical, they are not patentably distinct from each other because the scope of the rejected claims falls within the scope of the corresponding claims in the patent co-pending Application No. 09/163,993.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hyung S. Sough whose telephone number is (703) 308-0505. The Examiner can normally be reached Monday-Friday from 8:30 AM - 4:00 PM EST.

If attempts to reach the Examiner by telephone are unsuccessful, The Examiner's Supervisor, James P. Trammell, can be reached on (703) 305-9768.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703)305-3900. The Group Fax number is (703) 308-1396.

Hyung S. Sough
Primary Examiner
Art Unit 2161

shs
August 3, 2001